

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-162085

(43)Date of publication of application : 19.06.1998

(51)Int.Cl.

G06F 19/00

G07F 19/00

G07F 7/08

G09C 1/00

H04L 9/32

(21)Application number : 08-319146

(71)Applicant : N T T DATA TSUSHIN KK

(22)Date of filing : 29.11.1996

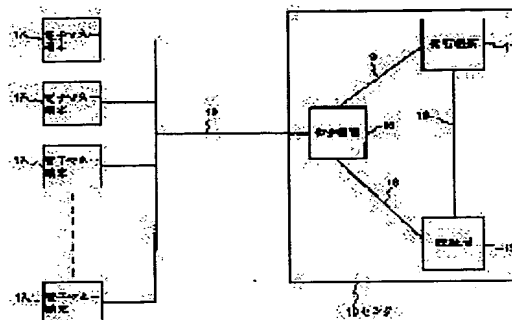
(72)Inventor : ICHIHARA NAOHISA  
YABUMOTO TAKESHI

## (54) ELECTRONIC MONEY SYSTEM, ELECTRONIC MONEY AND ELECTRONIC MONEY HISTORY GIVING METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an electronic money system that can hold the anonymity of a history content added to an electric money, the electronic money and an electronic money history giving method.

**SOLUTION:** An issuing institution 11, a certification bureau 13 and a mediation institution 15 are respectively provided with secret keys. History initial information (r) obtained by combining the secret keys is added to the electronic money. An electronic money terminal 17 receiving the electronic money converts history initial information (r) into history information (r) and transfers it to the other electronic money terminal 17. In the case of transfer from the other electronic money terminal 17, the electronic money terminal 17 adds its own user ID to the history information (r). For investigating the history of the electronic money, the mediation institution 15 subtracts the value of its own secret key from history information (r) of the returned electronic money and sends it to the issuing institution 11. The issuing institution 11 subtracts the value of the self-secret key from history information from the mediation institution 15, polynomial resolution is executed and the electronic money terminal to which the electronic money is transferred is specified.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平 1 0 - 1 6 2 0 8 5

(43)公開日 平成 1 0 年 ( 1 9 9 8 ) 6 月 1 9 日

(51) Int. Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G06F 19/00			G06F 15/30	360
G07F 19/00			G09C 1/00	660 C
7/08			G07D 9/00	476
G09C 1/00	660		G07F 7/08	Z
H04L 9/32			H04L 9/00	675 D

審査請求 未請求 請求項の数 1 8 O L (全 1 4 頁)

(21)出願番号 特願平 8 - 3 1 9 1 4 6

(22)出願日 平成 8 年 ( 1 9 9 6 ) 1 1 月 2 9 日

(71)出願人 0 0 0 1 0 2 7 2 8  
エヌ・ティ・ティ・データ通信株式会社  
東京都江東区豊洲三丁目 3 番 3 号

(72)発明者 市原 尚久  
東京都江東区豊洲三丁目 3 番 3 号 エヌ・  
ティ・ティ・データ通信株式会社内

(72)発明者 荻本 剛  
東京都江東区豊洲三丁目 3 番 3 号 エヌ・  
ティ・ティ・データ通信株式会社内

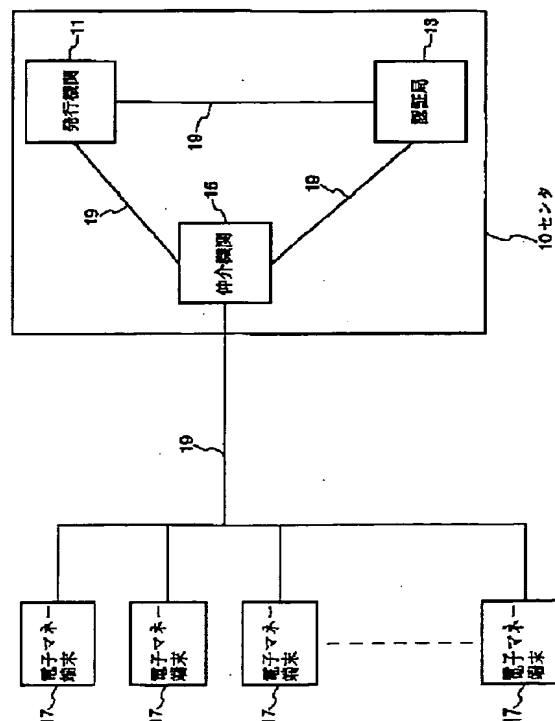
(74)代理人 弁理士 木村 満

(54)【発明の名称】 電子マネーシステム及び電子マネー及び電子マネー履歴付与方法

(57)【要約】

【課題】 電子マネーに付された履歴内容の匿名性が保持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法を提供する。

【解決手段】 発行機関 1 1 と認証局 1 3 と仲介機関 1 5 は、各自秘密鍵を備える。電子マネーには初めにそれらの秘密鍵を掛合わせた履歴初期情報  $r'$  を付す。その電子マネーを受信した電子マネー端末 1 7 は、所定式に従い、履歴初期情報  $r'$  を履歴情報  $r$  に変換し、他の電子マネー端末 1 7 に渡す。他の電子マネー端末 1 7 からの譲渡の場合、電子マネー端末 1 7 は、その履歴情報  $r$  に自己のユーザ ID を加える。電子マネーの履歴を調査する場合、仲介機関 1 5 は、戻されて来た電子マネーの履歴情報  $r$  から自己の秘密鍵の値を差し引き、発行機関 1 1 に送る。発行機関 1 1 は、仲介機関 1 5 からの履歴情報から自己の秘密鍵の値を差し引き、多項式分解し、その電子マネーが譲渡された電子マネー端末を特定する。



## 【特許請求の範囲】

【請求項 1】複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、

複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、

各前記端末には、自己を特定するための識別符号が付与されており、

各前記端末は、

受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第 1 の所定式に従って変換することにより自己の前記識別符号を含ませる第 1 の更新手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、を備え、

前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した 1 つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、

ことを特徴とする電子マネーシステム。

【請求項 2】前記センタから送信される電子マネーに付与されている前記履歴情報は、第 1 と第 2 と第 3 の鍵から構成されており、

前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報を前記第 1 の所定式に従って、前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項 1 に記載の電子マネーシステム。

【請求項 3】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第 1 と第 2 と第 3 の鍵のうちの前記 2 つの鍵の値を減算することにより、前記 1 つ又は複数の端末の識別符号の集合体を導出する手段を備え、

前記分解手段は、前記導出手段により導出された前記 1 つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備える、ことを特徴とする請求項 2 に記載の電子マネーシステム。

【請求項 4】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記分解手段は、前記電子マネーに付与されている前記

カウント情報を用いて前記集合体を多項式分解すること、ことを特徴とする請求項 3 に記載の電子マネーシステム。

【請求項 5】前記センタは、第 1 の鍵  $r_0$  を備える第 1 の制御手段と、第 2 の鍵  $r_1$  を備える第 2 の制御手段と、第 3 の鍵  $r_2$  を備える第 3 の制御手段と、前記第 1 と第 2 と第 3 の鍵から、数 1 で表される履歴情報  $r$  を算出する算出手段と、を備え、

前記端末に付与されている前記識別符号は 2 のべき乗値から構成され、

前記第 1 の所定式は、数 2 と数 3 を含み、

前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報  $r$  と数 2 に表す  $g(i)$  をもとに数 3 に表す式に従って  $r$  を更新する手段を備えることにより、数 4 に表す履歴情報  $r$  を導出する、

ことを特徴とする請求項 1 に記載の電子マネーシステム。

【数 1】  $r = r_0 \times r_1 \times r_2$

【数 2】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

( $b(r_i)$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 3】  $r = r \times g(i) \bmod N$

【数 4】  $r = r_0 + r_1 + x(i)$

【請求項 6】前記センタは、電子マネーを発行する発行機関と、前記電子マネーに付与する履歴情報を生成する認証局と、前記端末に前記電子マネーを供給する仲介機関とから構成され、

前記発行機関は、前記仲介機関及び端末に秘密の鍵である第 1 の鍵  $r_0$  を備え、

前記仲介機関は、前記発行機関及び端末に秘密の鍵である第 2 の鍵  $r_1$  を備え、

前記認証局は、前記仲介機関及び発行機関及び端末に秘密の鍵である第 3 の鍵  $r_2$  を備える、

ことを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の電子マネーシステム。

【請求項 7】前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報を前記第 1 の所定式に従って、前記複数の鍵から少なくとも 1 つを除いたものと該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項 1 に記載の電子マネーシステム。

【請求項 8】複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、

複数の鍵の積からなる履歴情報を作成して電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、

前記分解手段は、前記電子マネーに付与されている前記

各前記端末には、自己を特定するための識別符号が付されてお

り、

各前記端末は、

受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第 1 の所定式に従って変換することにより、前記複数の鍵の一部と自己の前記識別符号との和に変換する第 1 の更新手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、を備え、

前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した 1 つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、

ことを特徴とする電子マネーシステム。

【請求項 9】前記センタから送信される電子マネーに付与されている前記履歴情報は、第 1 と第 2 と第 3 の鍵から構成されており、

前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報を前記第 1 の所定式に従って、前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項 8 に記載の電子マネーシステム。

【請求項 10】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵の値を減算することにより、前記 1 つ又は複数の端末の識別符号の集合体を導出する手段を備え、

前記分解手段は、前記導出手段により導出された前記 1 つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備える、

ことを特徴とする請求項 9 に記載の電子マネーシステム。

【請求項 11】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解する、

ことを特徴とする請求項 8 乃至 10 のいずれか 1 項に記載の電子マネーシステム。

【請求項 12】前記センタは、電子マネーを発行する発行機関の鍵と、前記電子マネーに付与する前記履歴情報を生成する認証機関の鍵と、前記端末に前記電子マネー

を供給する仲介機関の鍵と、の積からなる初期履歴情報を電子マネーに付与する手段を備え、

前記第 1 の所定式は、前記初期履歴情報を前記発行機関と前記仲介機関との鍵とその端末の前記識別符号の和に変換する式である、

ことを特徴とする請求項 8 乃至 11 のいずれか 1 項に記載の電子マネーシステム。

【請求項 13】自己を特定するための識別符号が付されており、

10 電子マネーを受信する手段と、

受信した電子マネーの送信元を判別する判別手段と、

前記受信した電子マネーの送信元を電子マネーの供給元と判別した場合、該電子マネーに付与された履歴情報を第 1 の所定式に従って変換することにより、該履歴情報に自己の前記識別符号を含ませる第 1 の更新手段と、

前記受信した電子マネーの送信元を前記電子マネーの供給元以外であると判別した場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、

20 電子マネーを送信する手段と、

を備える端末から構成されることを特徴とする電子マネーシステム。

【請求項 14】前記電子マネーの供給元からの電子マネーには、数 5 に示す履歴情報  $r$  が付与されており、

前記第 1 の所定式は、数 6 と数 7 を含み、

前記第 1 の更新手段は、前記履歴情報  $r$  と数 6 に表す  $g(i)$  をもとに数 7 に表す式に従って  $r$  を更新する手段を備えることにより、数 8 に表す履歴情報  $r$  を導出する、

30 ことを特徴とする請求項 13 に記載の電子マネーシステム。

【数 5】  $r = r_0 \times r_1 \times r_2$ ;

ここで、 $r_0$  は電子マネーを発行する発行機関の鍵、 $r_1$  は前記電子マネーに付与する履歴情報を生成する認証局の鍵、 $r_2$  は前記端末に前記電子マネーを供給する仲介機関の鍵である。

【数 6】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

40  $(b(r_i))$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 7】  $r = r \times g(i) \bmod N$

【数 8】  $r = r_0 + r_1 + x(i)$

【請求項 15】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記端末は、受信した電子マネーに付されている前記カウント情報を更新する手段を含む、

50 ことを特徴とする請求項 13 又は 14 に記載の電子マネー

ーシステム。

・【請求項 1 6】識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネーであって、

・金銭的価値を有する情報と、

複数の鍵と該電子マネーが授受された端末の前記識別番号が含まれる履歴情報と、

該電子マネーが授受された端末の数をカウントするためのカウント情報と、より構成される、

ことを特徴とする電子マネー。

【請求項 1 7】識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネー取引の履歴を示す履歴情報を付与する電子マネー履歴付与方法であって、

複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給する供給ステップと、

前記端末が前記供給ステップより受信した前記電子マネーに付与された前記履歴情報を第 1 の所定式に従って該端末の識別符号を含むように変換する第 1 の更新ステップと、

前記端末が他の端末より受信した前記電子マネーに付与された前記履歴情報に該端末の識別符号を加える第 2 の更新ステップと、

前記端末からの前記電子マネーに付与された前記履歴情報を第 2 の所定式及び前記鍵を用いて変換することにより、該電子マネーが授受された 1 つ又は複数の端末の識別符号の集合体を導出するステップと、

前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解するステップと、

を備えることにより前記電子マネーが授受された全ての前記端末を特定することができることを特徴とする電子マネー履歴付与方法。

【請求項 1 8】第 1 の鍵  $r_0$  を記憶し、要求に応じて前記第 1 の鍵  $r_0$  を前記供給ステップに送信する第 1 の送信ステップと、

第 2 の鍵  $r_1$  を記憶し、要求に応じて前記第 2 の鍵  $r_1$  を前記供給ステップに送信する第 2 の送信ステップと、

第 3 の鍵  $r_2$  を記憶し、要求に応じて前記第 3 の鍵  $r_2$  を前記供給ステップに送信する第 3 の送信ステップと、を更に有し、

前記供給ステップは、前記第 1 と第 2 と第 3 の鍵から、数 9 に示される履歴情報  $r$  を算出して、前記電子マネーに付与し、

前記第 1 の更新ステップは、前記電子マネーに付与されている前記履歴情報  $r$  と数 1 0 に表す  $g(i)$  をもとに数 1 1 に表す式に従って  $r$  を更新することにより、数 1 2 に示す履歴情報  $r$  を導出する、

ことを特徴とする請求項 1 7 に記載の電子マネー履歴付与方法。

【数 9】  $r = r_0 \times r_1 \times r_2$ ;

【数 1 0】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

( $b(r_i)$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 1 1】  $r = r \times g(i) \bmod N$

【数 1 2】  $r = r_0 + r_1 + x(i)$

10 【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、電子マネーに履歴を付けることが可能な電子マネーシステムに関し、特に電子マネーに付された履歴の内容の匿名性を維持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法に関する。

【0 0 0 2】

【従来の技術】近年、金銭的価値を有する電子マネーを用いた電子マネーシステムが提案されている。このようなシステムにおいて電子マネーの不正使用が発見された場合、その流通経路を追跡するため、電子マネーに履歴を付けることが望ましい。その一例として、電子マネーに利用者の識別符号 (ID)、名前等を履歴として追加する方法が提案されている。しかし、この方法では、履歴を見ることにより、過去の使用者の ID、名前等が知られてしまうため、電子マネーの匿名性という機能が失われてしまう。

【0 0 0 3】

【発明が解決しようとする課題】本発明は、上記実状に鑑みてなされたもので、履歴内容の匿名性が維持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法を提供することを目的とする。

【0 0 0 4】

【課題を解決するための手段】上記目的を達成するため、この発明の第 1 の観点に係る電子マネーシステムは、複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、各前記端末には、自己を特定するための識別符号が付されており、各前記端末は、受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された履歴情報を第 1 の所定式に従って変換することにより自己の前記識別符号を含ませる第 1 の更新手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、を備え、前記センタは、前記端末からの電子マネー

に付与された前記履歴情報を第 2 の所定式及び前記鍵を用いて変換することにより、該電子マネーを授受した 1 つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える。

【 0 0 0 5 】このような構成によれば、電子マネーが授受された端末の識別符号を履歴情報として電子マネーに付与することができる。その際、端末は電子マネーの送信元を判別し、送信元に応じた履歴情報の付与方法を用いる。これにより、その電子マネーの履歴情報の初期値が第 1 の更新手段により変換されるため、その端末に再度、同電子マネーが譲渡されてもその履歴情報を見ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。また、電子マネーがセンタに戻されたとき、センタは、その電子マネーに付与された履歴から、鍵を用いて、前記端末の識別符号の集合体を導出し、その集合体を分解することにより、その電子マネーが授受された全ての端末を特定することができる。

【 0 0 0 6 】前記センタから送信される電子マネーに付与されている前記履歴情報は、第 1 と第 2 と第 3 の鍵から構成されてもよく、前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報を前記第 1 の所定式に従って、前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備えてもよい。

【 0 0 0 7 】このような構成によれば、端末は、センタから供給された電子マネーに付与されている前記第 1 と第 2 と第 3 の鍵からなる履歴情報を、前記第 1 の所定式を用いることにより、2 つの鍵と該端末の識別番号を付与した形に変換する。これにより、センタから初めに電子マネーを受け取った端末に、再度その電子マネーが譲渡されても、その端末は履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【 0 0 0 8 】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵の値を減算することにより、前記 1 つ又は複数の端末の識別符号の集合体を導出する手段を備えてもよく、前記分解手段は、前記導出手段により導出された前記 1 つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備えてもよい。例えば、前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解する。

【 0 0 0 9 】このような構成によれば、センタは端末からの履歴情報からその電子マネーが授受された端末の識別符号の集合体を導出し、その集合体をカウンタ情報を

用いて多項式分解することにより、各識別符号に分解する。これにより、ある電子マネーが授受された全ての端末と、各端末にその電子マネーが譲渡された回数とを特定することができる。よって、その電子マネーの履歴を知ることができる。

【 0 0 1 0 】例えば、前記センタは、第 1 の鍵  $r_0$  を備える第 1 の制御手段と、第 2 の鍵  $r_1$  を備える第 2 の制御手段と、第 3 の鍵  $r_2$  を備える第 3 の制御手段と、前記第 1 と第 2 と第 3 の鍵から、数 1 3 で表される履歴情報  $r$  を算出する算出手段と、を備え、前記端末に付与されている前記識別符号は 2 のべき乗値から構成され、前記第 1 の所定式は、数 1 4 と数 1 5 を含み、前記端末の前記第 1 の更新手段は、前記センタからの前記履歴情報  $r$  と数 1 4 に表す  $g(i)$  をもとに数 1 5 に表す式に従って  $r$  を更新（置換）する手段を備えることにより、数 1 6 に表す履歴情報  $r$  を導出する。

【数 1 3】  $r = r_0 \times r_1 \times r_2$ ;

【数 1 4】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

( $b(r_i)$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 1 5】  $r = r \times g(i) \bmod N$

【数 1 6】  $r = r_0 + r_1 + x(i)$

【 0 0 1 1 】このような構成によれば、ある端末がセンタから受信した電子マネーを再度他の端末から受信し、その電子マネーの以前の履歴情報  $r = r_0 \times r_1 \times r_2$  を記憶していたとしても、履歴情報  $r$  が  $r = r_0 + r_1 +$  (ユーザ ID の集合) と更新されており、 $r_0 + r_1$  の値が不明のため、履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【 0 0 1 2 】例えば、前記センタは、電子マネーを発行する発行機関と、前記電子マネーに付与する履歴情報を生成する認証局と、前記端末に前記電子マネーを供給する仲介機関とから構成され、前記発行機関は、前記仲介機関及び端末に秘密の鍵である第 1 の秘密鍵  $r_0$  を備え、前記仲介機関は、前記発行機関及び端末に秘密の鍵である第 2 の秘密鍵  $r_1$  を備え、前記認証局は、前記発行機関及び仲介機関及び端末に秘密の鍵である第 3 の秘密鍵  $r_2$  を備える。

【 0 0 1 3 】また、前記端末の前記第 1 の更新手段は、前記複数の鍵から構成される前記履歴情報を、該複数の鍵から少なくとも 1 つを除いたものと該端末の識別符号とより構成されるように更新してもよい。

【 0 0 1 4 】また、この発明の第 2 の観点に係る電子マネーシステムは、複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、複数の鍵の積からなる履歴情報を作成して電子マネーに付

10

20

30

40

50

与し、前記端末に該電子マネーを供給するセンタを備え、各前記端末には、自己を特定するための識別符号が付されており、各前記端末は、受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第 1 の所定式に従って変換することにより、前記複数の鍵の一部と自己の前記識別符号との和に変換する第 1 の更新手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、を備え、前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した 1 つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、ことを特徴とする。

【0015】このような構成によれば、第 1 の所定式により、センタの鍵の一部が履歴情報から除去されるので、同電子マネーが再びこの端末に送信された場合でも、この端末は電子マネーの流通の履歴を判別することができない。従って、電子マネーの匿名性を維持することができる。

【0016】前記センタから送信される電子マネーに付与されている前記履歴情報は、例えば、第 1 と第 2 と第 3 の鍵から構成されており、前記端末の前記第 1 の更新手段は、例えば、前記センタからの前記履歴情報を前記第 1 の所定式に従って、前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵と該端末の前記識別符号とより構成されるように更新する。

【0017】前記センタの前記導出手段は、例えば、前記端末からの前記履歴情報に含まれる前記第 1 と第 2 と第 3 の鍵のうちの 2 つの鍵の値を、該履歴情報から減算することにより、前記 1 つ又は複数の端末の識別符号の集合体を導出し、前記分解手段は、前記導出手段により導出された前記 1 つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する。

【0018】前記電子マネーに、該電子マネーが授受された端末の数を示すカウント情報を付与し、前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解するようにしてもよい。

【0019】前記センタは、例えば、電子マネーを発行する発行機関の鍵と、前記電子マネーに付与する前記履歴情報を生成する認証機関の鍵と、前記端末に前記電子マネーを供給する仲介機関の鍵と、の積からなる初期履歴情報を電子マネーに付与する手段を備え、前記第 1 の所定式は、前記初期履歴情報を前記発行機関と前記仲介機関との鍵とその端末の前記識別符号の和に変換する式

である。

【0020】また、この発明の第 3 の観点に係る電子マネーシステムは、自己を特定するための識別符号が付されており、電子マネーを受信する手段と、受信した電子マネーの送信元を判別する判別手段と、前記受信した電子マネーの送信元を電子マネーの発行元と判別した場合、該電子マネーに付与された前記履歴情報を第 1 の所定式に従って変換することにより、該履歴情報に自己の前記識別符号を含ませる第 1 の更新手段と、前記受信した電子マネーの送信元を電子マネーの発行元以外と判別した場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第 2 の更新手段と、電子マネーを送信する手段と、を備える、ことを特徴とする。

【0021】このような構成によれば、電子マネーが授受される際、その電子マネーに履歴情報を付与することができる。また、このシステムでは、受信した電子マネーの送信元を判別し、送信元が電子マネーの発行元の場合、その電子マネーの履歴情報を第 1 の所定式に従って更新して送信する。これにより、その電子マネーの履歴情報の初期値が変わるため、再度、同電子マネーが譲渡されても、その履歴情報を見ることは不可能となる。よって、匿名性を保持した電子マネーシステムを実現することができる。

【0022】例えば、電子マネーの供給元からの電子マネーには、数 17 に示す履歴情報  $r$  が付与されており、前記第 1 の所定式は、数 18 と数 19 を含んでもよく、前記第 1 の更新手段は、前記履歴情報  $r$  と数 18 に表す  $g(i)$  をもとに数 19 に表す式に従って前記履歴情報  $r$  を更新する手段を備えることにより、数 20 に示す履歴情報  $r$  を導出するようにしてもよい。

【0023】

【数 17】  $r = r_0 \times r_1 \times r_2$

【数 18】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

( $b(r_i)$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 19】  $r = r \times g(i) \bmod N$

【数 20】  $r = r_0 + r_1 + x(i)$

【0024】このような構成によれば、電子マネーの送信元が電子マネーの発行元である場合、前記第 1 の更新手段により、その電子マネーの履歴情報の初期値から秘密鍵  $r_2$  の値を差し引いた値が新たな履歴情報として電子マネーに付与される。これにより、その電子マネーの履歴情報の初期値が変わるため、再度、同電子マネーが譲渡されても、その履歴情報を見ることは不可能となる。よって、匿名性を保持した電子マネーシステムを実現することができる。

【0025】また、この発明の第 4 の観点に係る電子マ

ネーは、識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネーであって、金銭的価値を有する情報と、複数の鍵と該電子マネーが授受された端末の前記識別番号が含まれる履歴情報と、該電子マネーが授受された端末の数をカウントするためのカウント情報と、より構成される。

【 0 0 2 6 】これにより、その電子マネーが授受された端末を特定することができる。

【 0 0 2 7 】また、この発明の第 5 の観点に係る電子マネー履歴付与方法は、識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネー取引の履歴を示す履歴情報を付与する電子マネー履歴付与方法であって、複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給する供給ステップと、前記端末が前記供給ステップより受信した前記電子マネーに付与された前記履歴情報を第 1 の所定式に従って該端末の識別符号を含むように変換する第 1 の更新ステップと、前記端末が他の端末より受信した前記電子マネーに付与された前記履歴情報に該端末の識別符号を加える第 2 の更新ステップと、前記端末からの前記電子マネーに付与された前記履歴情報を第 2 の所定式及び前記鍵を用いて変換することにより、該電子マネーが授受された 1 つ又は複数の端末の識別符号の集合体を導出するステップと、前記 1 つ又は複数の端末の識別符号の集合体を各識別符号に分解するステップと、を備えることにより前記電子マネーが授受された全ての前記端末を特定することができることを特徴とする。

【 0 0 2 8 】これにより、電子マネーが授受された端末の識別符号を履歴として付与することができる電子マネーシステムを実現することができる。また第 1 の更新ステップにより、その電子マネーの履歴情報の初期値が変換されるため、同端末に再度、同電子マネーが譲渡されてもその履歴情報を見ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。また、端末が電子マネーの送信元を判別し、送信元に応じた履歴の付与方法を用いることにより、センタに電子マネーが戻されたとき、所定の方法を用いて、その電子マネーが授受された全ての端末を特定することができる。

【 0 0 2 9 】第 1 の鍵  $r_0$  を記憶し、要求に応じて前記第 1 の鍵  $r_0$  を前記供給ステップに送信する第 1 の送信ステップと、第 2 の鍵  $r_1$  を記憶し、要求に応じて前記第 2 の鍵  $r_1$  を前記供給ステップに送信する第 2 の送信ステップと、第 3 の鍵  $r_2$  を記憶し、要求に応じて前記第 3 の鍵  $r_2$  を前記供給ステップに送信する第 3 の送信ステップと、を更に有してもよく、前記供給ステップは、前記第 1 と第 2 と第 3 の鍵から、数 2 1 に示される履歴情報  $r$  を算出して、前記電子マネーに付与し、前記

第 1 の更新ステップは、前記電子マネーに付与されている前記履歴情報  $r$  と数 2 2 に表す  $g(i)$  をもとに数 2 3 に表す式に従って  $r$  を更新することにより、数 2 4 に示す履歴情報  $r$  を導出してもよい。

【 0 0 3 0 】

【数 2 1】  $r = r_0 \times r_1 \times r_2$ ;

【数 2 2】  $g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_1) \times b(r_2))$

( $b(r_i)$  は  $r_i$  の関数であり  $r_i \times b(r_i) \bmod N = 1$  を満たす。なお、 $N$  は定数であり、 $A \bmod B$  は、 $A$  を  $B$  で割った余りを示す。 $x(i)$  は、任意の端末  $i$  の識別符号を示す。)

【数 2 3】  $r = r \times g(i) \bmod N$

【数 2 4】  $r = r_0 + r_1 + x(i)$

【 0 0 3 1 】これにより、前記供給手段より受信した電子マネーには、前記第 1 の更新ステップにより、その電子マネーの履歴情報の初期値から鍵  $r_2$  の値を差し引いた値が新たな履歴情報として付与される。これにより、電子マネーの履歴情報の初期値が変わるため、前記供給ステップから初めにその電子マネーを受信した端末が、再度、同電子マネーを受信しても、その履歴情報を見ることができない。よって、匿名性を保持した電子マネーシステムを実現することができる。

【 0 0 3 2 】

【発明の実施の形態】本発明の実施の形態に係る電子マネーシステムについて、以下図面を参照して説明する。この電子マネーシステムは、図 1 に示すように、電子マネーの発行機関 1 1 と認証局 1 3 と仲介機関 1 5 とを備えるセンタ 1 0 と、複数の電子マネー端末 1 7 と、これらを接続する通信網 1 9 より構成される。このシステムでは、発行機関 1 1 により発行された電子マネーが仲介機関 1 5 を介して利用者の電子マネー端末 1 7 に供給され、利用者の電子マネー端末 1 7 の間で電子マネーがやり取りされる形態をとる。

【 0 0 3 3 】発行機関 1 1 は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータを備え、電子マネーの発行、後述する履歴の調査等を行う。発行機関 1 1 は、各電子マネー端末 1 7 を特定するためのユーザ ID のテーブルを記憶する。また、発行機関 1 1 は、システム公開鍵  $N$  を生成し、各利用者の電子マネー端末 1 7 に通信網 1 9 を介して配布する。認証局 1 3 は、発行機関 1 1 により発行された電子マネーに付与する履歴の初期情報（履歴初期情報）の生成等を行うコンピュータを備える。

【 0 0 3 4 】仲介機関 1 5 は、例えば、金融機関等に設置され、発行機関 1 1 との電子マネーの売買、利用者と電子マネーの売買等を行うコンピュータを備える。電子マネー端末 1 7 は、利用者が仲介機関 1 5 と電子マネーを売買し、他の利用者と電子マネーをやり取りするための端末である。各電子マネー端末 1 7 は、システム公



開鍵N、ユーザID、履歴を更新するためのプログラム等を記憶する。また、発行機関11は $r_0$ 、認証局13は $r_1$ 、仲介機関15は $r_2$ をそれぞれ認証局13を除く他者に秘密な鍵(秘密鍵)として保持する。なお、 $r_0$ と $r_1$ と $r_2$ は素数とする。

【0035】本システムにおいて電子マネーの売買は通信を介して行われ、その精算方法は任意である。例えば、図2に示すように、このシステムの電子マネー端末17と仲介機関15と発行機関11の決済口座を有する金融機関のコンピュータが通信網19に接続されている。この金融機関のコンピュータが、電子マネーの売買が行われると、買い手の決済口座から売り手の決済口座へ売買された電子マネー相当の金額を振り替えるようにしてもよい。

【0036】例えば、仲介機関15が電子マネー端末17からの要求に回答して3万円分の電子マネーを送信した場合、金融機関のコンピュータは、電子マネー端末17の決済口座から仲介機関15の決済口座へ3万円を振り替える。また、電子マネー端末17が仲介機関15へ1万円分の電子マネーを送信した場合、金融機関のコンピュータは、仲介機関15の決済口座から電子マネー端末17の決済口座へ1万円を振り替える。また、発行機関11が仲介機関15からの要求に回答して20万円分の電子マネーを送信した場合、金融機関のコンピュータは、仲介機関15の決済口座から発行機関11の決済口座へ20万円を振り替える。また、仲介機関15が発行機関11へ10万円分の電子マネーを送信した場合、金融機関のコンピュータは、発行機関11の決済口座から仲介機関15の決済口座へ10万円を振り替える。

【0037】仲介機関15が各利用者の電子マネー端末17に供給する電子マネーの初期化处理について図3を参照して説明する。仲介機関15は、例えば、予め一定額の電子マネーを発行機関11から購入しておく。電子マネー端末17は、仲介機関15から電子マネーを購入したい場合、仲介機関15に金額、ユーザID等を含む電子マネー購入要求を送信する。仲介機関15は、この電子マネー購入要求に回答して、電子マネーに付与する履歴初期情報を作成するため、発行機関11に秘密鍵 $r_0$ を認証局13に送信するよう指示する(L1)と共に、自己の秘密鍵 $r_1$ を認証局13に送信する(L2)。発行機関11は、仲介機関15からの指示を受けて、自己の秘密鍵 $r_0$ を認証局13に送信する(L3)。なお、発行機関11は、秘密鍵 $r_0$ を予め認証局13に送信しておいても良い。

【0038】認証局13は、受信した秘密鍵 $r_0$ 、 $r_1$ と自己の秘密鍵 $r_2$ をもとに、電子マネーに付与する履歴の初期情報である履歴初期情報 $r' = r_0 \times r_1 \times r_2$ を算出し、仲介機関15に送信する(L4)。仲介機関15は、受信した履歴初期情報 $r'$ と、電子マネーの利用

者の数をカウントするためのカウンタ情報 $c$ (初期値0に設定)とを、図4に示すように、発行機関11により発行された電子マネーに付加する。これにより、電子マネーの初期化处理が完了する。初期化处理完了後、仲介機関15は、履歴情報が付与された電子マネーを要求元の電子マネー端末17に送信する。

【0039】次に、各電子マネー端末17における電子マネーに付加された履歴の更新処理について説明する。まず、前提として、各利用者の電子マネー端末17( $i = 1, 2, \dots, m$ ( $m$ は端末総数))が記憶するユーザIDを2のべき乗値である $x(i)$ とし、電子マネー端末17が電子マネーを仲介機関15から受信した際にその履歴初期情報 $r'$ を履歴情報 $r$ に更新するための更新式を $g(i)$ とすると、それらは数25、数26の様に示される。

【0040】

【数25】 $x(i) = 2^k$  ( $k \geq 0$ )

【数26】 $g(i) = r_2^{-1} \times (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1} \cdot r_1^{-1})$  ( $1 \leq i \leq m$ )

但し、任意の数 $a$ とした場合、 $a^{-1}$ は、 $a \cdot a^{-1} \bmod N = 1$ を満たし、 $A \bmod B$ は、 $A$ を $B$ で割った余りを示す。

【0041】まず、電子マネー端末17が、仲介機関15から電子マネーを購入した場合、電子マネー端末17は、履歴情報 $r$ を数27に従って算出し、カウンタ情報 $c$ を1カウントアップ( $c = c + 1$ )して、図5に示すように、電子マネーに付加する。

【0042】

【数27】 $r = r' \times g(i) \bmod N$

これにより、仲介機関15から電子マネー端末17に受け渡された電子マネーの履歴に、その電子マネー端末17のユーザIDを付加することができる。

【0043】電子マネー端末17が、他の電子マネー端末17から電子マネーを受け取った場合、電子マネー端末17は、その電子マネーに付与されている履歴情報 $r$ に自己のユーザIDである $x(i)$ を足し込み、カウンタ情報 $c$ を1カウントアップする。即ち、電子マネー端末17は、

(新たな履歴情報 $r$ ) = (前回の履歴情報 $r$ ) +  $x(i)$

(新たなカウンタ情報 $c$ ) = (前回のカウンタ情報 $c$ ) + 1

に従って計算し、その電子マネーの履歴を更新する。これにより、電子マネー端末17が、他の電子マネー端末17から受け取った電子マネーの履歴に、その電子マネー端末17のユーザIDが付加される。

【0044】仲介機関15から受け取った電子マネーの履歴初期情報 $r'$ に、各電子マネー端末17がユーザIDを加えていくだけの場合、最初に電子マネーを受け取る電子マネー端末17が、その電子マネーの履歴初期情報 $r'$ を知ることができるため、再度その電子マネーを

受け取ったとき、その電子マネーの履歴内容を知ることができてしまう。

【0045】例えば、図6に示すように履歴初期情報  $r' = 10$  の電子マネーが仲介機関15から電子マネー端末17aに渡った場合、電子マネー端末17aは履歴初期情報  $r' = 10$  を記憶しておき、他の電子マネー端末17bに渡す。その後も幾度かの譲渡を経て、再び電子マネー端末17aにその電子マネーが渡された場合、電子マネー端末17aは、受け取った電子マネーの履歴情報  $r$  から自己が記憶する履歴初期情報  $r' = 10$  を差

$$\begin{aligned} r &= r' \times g(i) \bmod N \\ &= r_0 \cdot r_1 \cdot r_2 \times r_2^{-1} \cdot (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1}) \\ &= r_0 \cdot r_1 \cdot (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1}) \\ &= r_0 + r_1 + x(i) \end{aligned}$$

【0048】つまり、図7に示すように、最初に仲介機関15から電子マネーを受け取った電子マネー端末17aが上記の式を用いて履歴情報を更新することにより、電子マネー端末17aがその後再びその電子マネーを受け取っても、 $r_0 + r_1$  の値がわからないため、履歴内容を知ることができない。これにより、電子マネーの匿名性を保持することができる。

【0049】例えば、電子マネー端末17から仲介機関15に戻された電子マネーの不正使用が検出された場合、その電子マネーの流通経路を追跡するために、その電子マネーの履歴を調べる必要がある。このような場合での電子マネーの履歴の調査処理について、以下説明する。まず、仲介機関15は、受信した電子マネーに付加されている履歴情報  $r$  から自己の秘密鍵  $r_1$  の値を差し引いた値  $(r - r_1)$  とカウンタ情報  $c$  を発行機関11

$$\begin{aligned} r - r_1 - r_0 &= (r_0 + r_1 + x(i) + \dots + x(n)) - r_1 - r_0 \\ &= x(i) + \dots + x(n) \end{aligned}$$

なお、各ユーザID  $x(i)$ 、 $\dots$ 、 $x(n)$ は、2のべき乗値なので、数30に示すように表せる。

【0053】

【数30】

$$x(i) + \dots + x(n) = \sum_{h=0}^n a(h) \times 2^h$$

また、カウンタ情報  $c$  は、数31に示すように表せる。

【0054】

【数31】

$$c = \sum_{h=0}^n a(h)$$

【0055】数30、数31より  $a(h)$  を一意に決定することができ、この各  $a(h)$  が、この電子マネーを電子マネー端末17<sub>1</sub>、 $\dots$ 、17<sub>n</sub>のそれぞれが受け取った回数となる。これにより発行機関11は、「どの電子マネー端末17が何回この電子マネーを受け取ったのか」を知ることができる。

【0056】また、仲介機関15に関しても、仮に仲介

し引き、カウンタ情報  $c$  を用いて多項式分解することにより、その電子マネーを利用した利用者の電子マネー端末17のユーザIDを知ることができてしまう。

【0046】しかし、この発明の電子マネーシステムでは、電子マネー端末17<sub>1</sub>が仲介機関15から電子マネーを受け取った際に行う履歴情報  $r$  の算出式を展開すると数28に示すようになる。

【0047】

【数28】

に送る。

【0050】発行機関11は、受信した電子マネーに付与された履歴情報  $(r - r_1)$  から自己の秘密鍵  $r_0$  の値を差し引き、カウンタ情報  $c$  を用いて多項式分解する。発行機関11は、多項式分解により導出した分解要素集合を履歴  $V$  とし、この履歴  $V$  に含まれる各要素  $v \in V$  をユーザIDとして求める。

【0051】発行機関11の多項式分解処理について詳しく説明する。発行機関11は、仲介機関15から受信した履歴情報  $(r - r_1)$  から自己の秘密鍵  $r_0$  の値を更に差し引く。これにより、数29に示すように、この電子マネーを利用した各利用者のユーザIDを足し込んだものが導出される。

【0052】

【数29】

機関15がその電子マネーの履歴初期情報  $r'$  ( $= r_0 \times r_1 \times r_2$ ) を記憶していても、それから  $r_0$  を求めることはできないため、自己に渡された電子マネーの履歴を知ることはできない。よって、本システムでは、発行機関11のみが仲介機関15の協力を受けて電子マネーの履歴内容を知ることができる。

【0057】発行された電子マネーが仲介機関15から電子マネー端末17に渡り、幾度かの譲渡を経て仲介機関15に戻り、発行機関11によってその履歴内容が導出されるまでの処理を図8を参照して具体的に説明する。例えば、端末数を3（電子マネー端末17<sub>1</sub>、17<sub>2</sub>、17<sub>3</sub>）、秘密鍵  $r_0 = 7$ 、秘密鍵  $r_1 = 3$ 、秘密鍵  $r_2 = 5$ 、システム公開鍵  $N = 419$ 、とする。これらの条件により、 $r_0^{-1} = 60$ 、 $r_1^{-1} = 140$ 、 $r_2^{-1} = 84$  と決定され、ユーザIDである  $x(i)$  と、更新式である  $g(i)$  は表1に示す様に決定される。

【0058】

【表1】

17

18

電子マネー端末17 <sub>i</sub>	$x(i)$	$g(i)$
電子マネー端末17 <sub>1</sub>	$x(1)=1=2^0$	$g(1)=722400$
電子マネー端末17 <sub>2</sub>	$x(2)=2=2^1$	$g(2)=1428000$
電子マネー端末17 <sub>3</sub>	$x(3)=4=2^2$	$g(3)=2839200$

【0059】例えば、電子マネー端末17<sub>i</sub>が仲介機関15に電子マネー要求信号を送信する(S0)。仲介機関15は、この電子マネー要求信号に応答して、発行機関11に秘密鍵を認証局13に送信するよう指示する(S1)と共に、自己の秘密鍵 $r_i=3$ を認証局13に送信する(S2)。発行機関11は、仲介機関15からの指示に応答して、自己の秘密鍵 $r_i=7$ を認証局13に送信する(S3)。

【0060】認証局13は、自己の秘密鍵 $r_i=5$ を用いて、履歴初期情報 $r'=r_i \times r_i \times r_i=7 \times 3 \times 5=105$ を計算し(S4)、仲介機関15に送信する(S5)。仲介機関15は、受信した履歴初期情報 $r'$ と、カウンタ情報 $c=0$ を電子マネーMに付加する。

【0061】仲介機関15は、要求信号を受信すると、履歴初期情報 $r'$ とカウンタ情報 $c=0$ が付与された電子マネーMを電子マネー端末17<sub>i</sub>に送信する(S6)。電子マネー端末17<sub>i</sub>は、仲介機関15から電子マネーMを受信し、その電子マネーMに付与されている履歴初期情報 $r'$ とカウンタ情報 $c$ に対して、数32と数33に示す計算を行うことにより、履歴初期情報 $r'$ を履歴情報 $r$ に更新し、 $c$ を1カウントアップする(S7)。

【0062】

【数32】 $r=r' \times g(2) \bmod N=105 \times 1428000 \bmod 419=12$

【数33】 $c=0+1=1$

【0063】次に、電子マネー端末17<sub>i</sub>は、その電子マネーMを電子マネー端末17<sub>j</sub>に譲渡することとする。電子マネー端末17<sub>i</sub>は、電子マネー端末17<sub>j</sub>から受信した電子マネーに付与されている履歴情報 $r$ とカウンタ情報 $c$ を数34と数35に示す様に更新する(S8)。

【0064】

【数34】 $r=r+x(1)=12+1=13$

【数35】 $c=1+1=2$

【0065】次に、電子マネー端末17<sub>i</sub>は、その電子マネーMを電子マネー端末17<sub>k</sub>に譲渡することとする。電子マネー端末17<sub>i</sub>は、電子マネー端末17<sub>k</sub>から受信した電子マネーに付与されている履歴情報 $r$ とカウンタ情報 $c$ を数36と数37に示す様に更新する(S9)。

【0066】

【数36】 $r=r+x(3)=13+4=17$

【数37】 $c=2+1=3$

【0067】最後に、電子マネー端末17<sub>i</sub>は、その電子マネーMを電子マネー端末17<sub>j</sub>に譲渡することとする。電子マネー端末17<sub>i</sub>は、電子マネー端末17<sub>j</sub>から受信した電子マネーに付与されている履歴情報 $r$ とカウンタ情報 $c$ を数38と数39に示す様に更新する(S10)。

【0068】

【数38】 $r=r+x(2)=17+2=19$

【数39】 $c=3+1=4$

【0069】電子マネー端末17<sub>i</sub>は、電子マネーMを換金するため仲介機関15に送信する(S11)。例えば、仲介機関15が電子マネーMを受信した際、不正検出等の理由により、その電子マネーMの履歴を調べる必要が発生したとする。この場合、仲介機関15は、電子マネーMの履歴情報 $r$ から自己の秘密鍵 $r_i$ の値を差し引いて( $r=19-3=16$ )(S12)、電子マネーMを履歴調査要求と共に発行機関11に送信する(S13)。

【0070】発行機関11は、受信した履歴調査要求に応答して、電子マネーMの履歴情報 $r$ から自己の秘密鍵 $r_i$ の値を差し引いて、 $r=16-7=9$ と算出する。この算出結果が、電子マネーMが譲渡された各電子マネー端末17のユーザIDの集合となる。発行機関11は、 $r=9$ とカウンタ情報 $c=4$ と自己が記憶するユーザIDテーブル(表1)を用いて数40に示す様に多項式分解する(S14)。即ち、 $r$ の値を、項数が $c$ で、各項の値が $x(i)$ のいずれかとなるように多項式分解する。

【0071】

【数40】 $r=9=1+2+2+4$ 表1より、 $x(1)=1$ 、 $x(2)=2$ 、 $x(3)=4$ なので、「この電子マネーMは、電子マネー端末17<sub>i</sub>に1回、電子マネー端末17<sub>j</sub>に2回、電子マネー端末17<sub>k</sub>に1回譲渡されて仲介機関15に戻ってきた」という履歴の調査結果が得られる。

【0072】なお、各電子マネー端末17のユーザIDである $x(i)$ 、更新式 $g(i)$ の取得方法は任意である。例えば、電子マネー端末17がこのシステムのユーザ登録をする際に、発行機関11が、その電子マネー端末17に対して新たなユーザIDである $x(n)$ を生成し、そのユーザIDである $x(n)$ と自己の秘密鍵 $r_i$ を認証局13に送信すると共に、仲介機関15に秘密鍵 $r_i$ を認証局13に送信するよう指示する。

【0073】認証局13は、受信した秘密鍵 $r_i$ 、 $r_i$ と

ユーザ ID である  $x(n)$  をもとに更新式  $g(n)$  を算出し、ユーザである ID  $(n)$  とともに発行機関 11 に送信する。発行機関 11 は、通信網 19 を介して、ユーザ登録する電子マネー端末 17 にユーザ ID である  $x(n)$  と更新式  $g(n)$  を送信する。電子マネー端末 17 は、受信したユーザ ID である  $x(n)$  と更新式  $g(n)$  を記憶する。

【0074】上記説明では、3つの秘密鍵  $r_0$ 、 $r_1$ 、 $r_2$  を用いたが、秘密鍵の数はこれに限定されず任意である。

【0075】なお、電子マネー端末 17 の形態は任意であり、個人・商店の取引用端末 (POS)、移動端末 (モバイル端末) 等でもよい。

【0076】また、電子マネー端末 17 は、着脱可能な IC カードを備えてもよく、この IC カードに、ユーザ ID である  $x(i)$ 、更新式  $g(i)$ 、残高等を記憶してもよい。利用者が電子マネー端末 17 を使用する時以外はこの IC カードを他の場所に保管しておくことにより、セキュリティを高めることができる。このとき、例えば、書き換え不可能な追記型の光記憶部と、IC メモリ部とを備えた IC カードを用いてもよい。この場合、IC メモリ部に残高等を記憶し、光記憶部に電子マネーのチャージ、支払い、譲渡、換金等の履歴を追記することが望ましい。

【0077】なお、この発明の電子マネーシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体 (フロッピーディスク、CD-ROM 等) から該プログラムをインストールすることにより、上述の処理を実行するコンピュータ及び端末を構成することができる。

【0078】また、コンピュータにプログラムを供給するための媒体は、通信媒体 (通信回線、通信ネットワーク、通信システムのように、一時的に流動的にプログラムを保持する媒体) でも良い。例えば、通信ネットワークの掲示板 (BBS) に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OS の制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処

理を実行することができる。

【0079】

【発明の効果】以上説明したように、本発明によれば、端末が電子マネーを供給するコンピュータから電子マネーを受け取った際、その電子マネーに付与されている複数の秘密鍵からなる履歴情報を、複数の秘密鍵のうちのいくつかと該端末の識別番号より構成されるように変換させる。これにより、該端末が、再度その電子マネーを受け取っても、履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図 2】電子マネーを売買する際の精算方法の一例を説明するための図である。

【図 3】電子マネーの初期化処理を説明するための図である。

【図 4】仲介機関により初期化処理された電子マネーの構成を示す図である。

【図 5】電子マネー端末が仲介機関から受信した電子マネーに対して更新処理したときの電子マネーの構成を示す図である。

【図 6】電子マネーの履歴初期情報に各電子マネー端末のユーザ ID を加えていくだけの履歴の更新処理について説明するための図である。

【図 7】本発明の電子マネーシステムにおける履歴の更新処理を説明するための図である。

【図 8】発行された電子マネーが、複数の電子マネー端末間において譲渡され、仲介機関に戻され、発行機関によってその履歴内容が導出されるまでの処理を具体的に説明するための図である。

【符号の説明】

- 11 発行機関
- 13 認証局
- 15 仲介機関
- 17 電子マネー端末
- 19 通信網

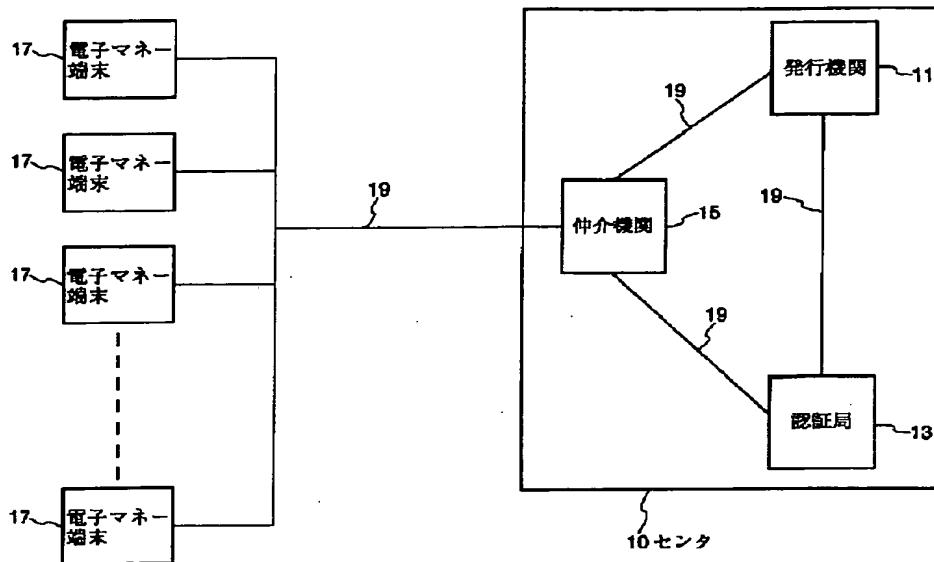
【図 4】

電子マネー	履歴初期情報	カウンタ情報
	$r = r_0 \times r_1 \times r_2$	$c = 0$

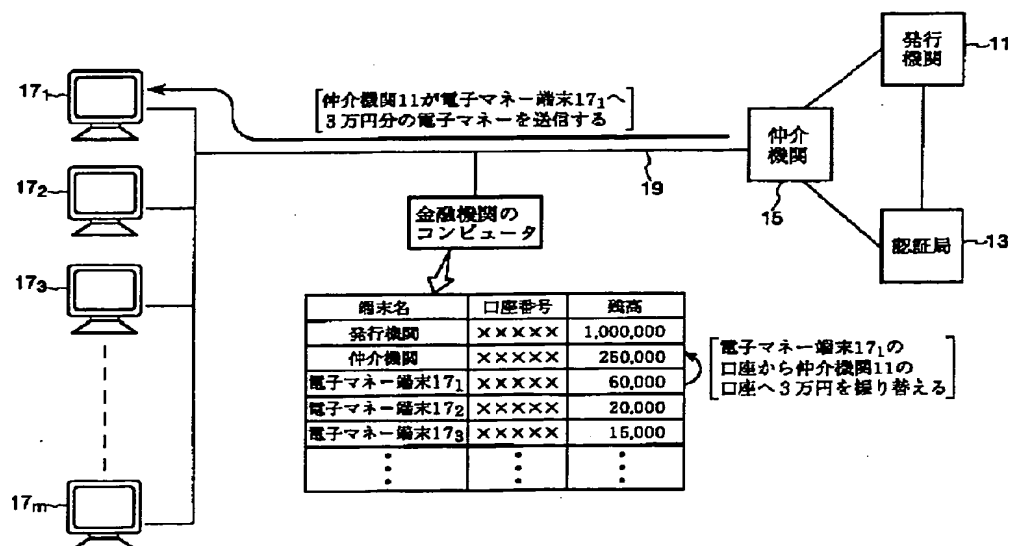
【図 5】

電子マネー	履歴情報	カウンタ情報
	$r = r \times g(i) \bmod N$	$c = 1$

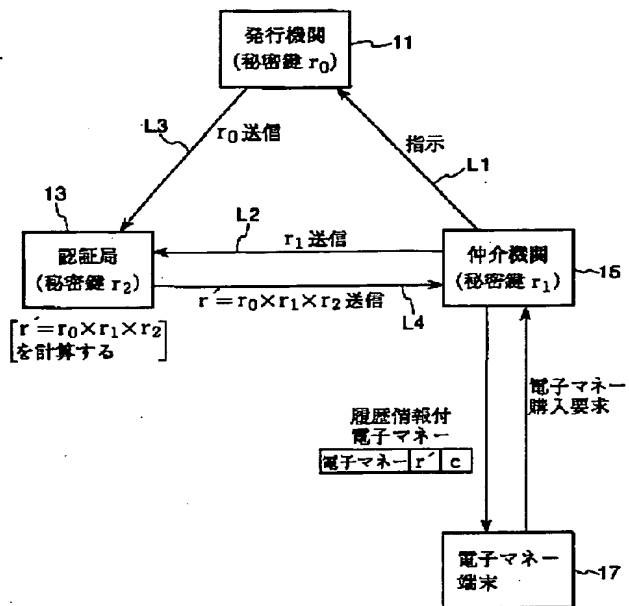
【 図 1 】



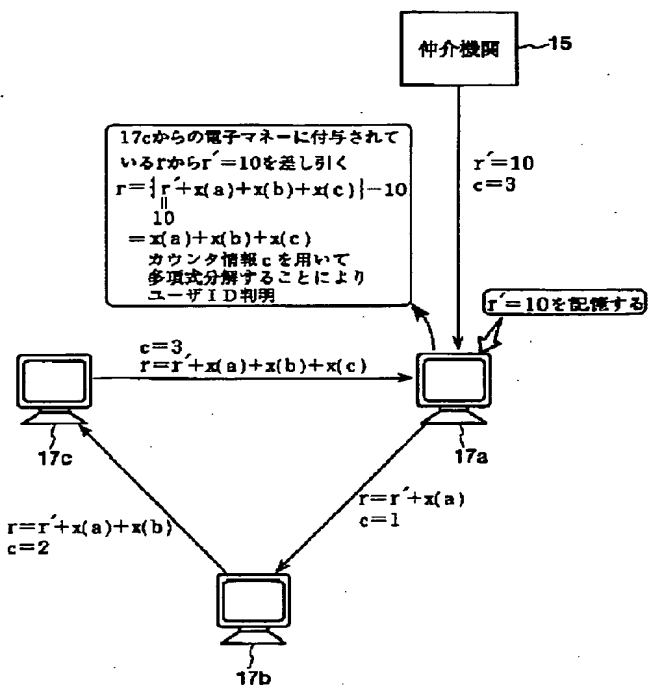
【 図 2 】



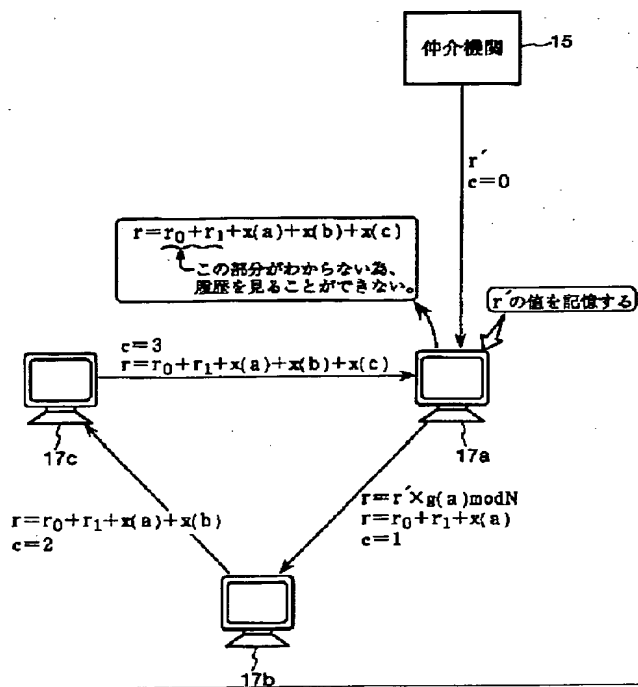
【 図 3 】



【 図 6 】

〈電子マネー端末が単純に $x(i)$ を付加する場合〉

【 図 7 】



【 図 8 】

